**TELKOMNIKA**, Vol.17, No.6, December 2019, pp.2812~2817
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
**DOI:** 10.12928/TELKOMNIKA.v17i6.12490


# A brief review: security issues in cloud computing and their solutions

**Iqbal Ahmed**
Department of Computer Science and Engineering, University of Chittagong,
Chittagong-4331, Bangladesh
*Corresponding author, e-mail: iqbal.ahmed@cu.ac.bd

*Cloud computing is an Internet-based, emerging technology, tends to be prevailing in our environment especially in the field of computer sciences and information technologies which require network computing on large scale. Cloud Computing is a shared pool of services which is gaining popularity due to its cost, effectiveness, avilability and great production. Along with its numerous benefits, cloud computing brings much more challenging situation regarding data privacy, data protection, authenticated access, Intellectual property rights etc. Due to these issues, adoption of cloud computing is becoming difficult in today's world. In this review paper, various security issues regarding data privacy and reliability, key factors which are affecting cloud computing, have been addressed and also suggestions on particular areas have been discussed.*

***Keywords***: *cloud computing, cloud security, data encryption, data protection, digital signature*



## 1. Introduction

Cloud computing is a service that is internet based and that gives the facility of sharing computer resources along with other devices on user demand. It is a mechanism to enable on demand shared resources. For example, server, data centre, networks, storage applications which can store data. That can be generated with minimum effort. In addition, cloud computing provides the facility to the organizations and users to keep their data on private or third-party storage location and these locations/data centres may be located far away from user, may be in some other city or country in this world. National Institute of Standard and Technology (NIST) gives the cloud computing's definition as cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1, 2]. For better understanding of cloud computing services, one needs to comprehend the importance and characteristics of cloud services which are explained here and represented in Figure 1 [3]:

- On demand Self-service: It refers to the service which enables provisioning of cloud resources to vendors on demand or whenever they are required such as network storage, service time without human interaction.
- Broad Network Access: Services are accessible over the network which are retrieved through some standardized mechanism which promotes the usages of heterogeneous platforms (workstations, tablets, laptops, mobile phones).
- Resource Pooling: Resources of cloud provider are pooled over the server. Consumers are assigned different resources which are either physical or virtual one. Generally, consumers have no idea of exact location the resources provided to them except at the abstraction level like state, city, country or data centre.
- Rapid Elasticity: Services can be elastically released and monitored for consumers services available to them can often appear as unlimited which can be scaled in quantity anytime.
- Measured Services: Cloud system are so designed that they can monitor the resource usages, for example processing, bandwidth and active user accounts, storage to deliver transparency to provider as well as consumer. At some level of abstraction, they can optimize the resource usage by keeping a check through metering capability.

*Received February 5, 2019; Revised June 6, 2019; Accepted July 2, 2019*

This paper is divided into following sections: section 1 tells about the introduction of cloud computing, section 2 gives the idea of cloud computing models while section 3 is the brief introduction of related works. Section 4 is about the factors affecting cloud computing, section 5 is the possible threats regarding the cloud computing paradigm and finally section 6 gives some solutions to the security issues. The conclusive remark is in section 7.

## 2. Cloud Service Models

The benefits and impotence of cloud computing might be very appealing and demandable, but it has got huge number of risks and security issues like data leakage, data loss, intruder attacks, malicious insiders etc. Following service models are defined by NIST which includes three categories [1, 3, 4]:

- Infrastructure as a Service (IaaS): IaaS is all about providing the virtual machine, operating systems or networks to the end users. Some other computing resources are also supported in IaaS, where the customer or client can run arbitrary operating system on virtual machine or any other software. Client can control only the operating system or software which he is running but he loses his control on the infrastructure which is providing him all these services.
- Software as a Service (SaaS): In this kind of scenario, user is only using the applications which are being provided by the vendor and those applications run on the cloud services. Same application is accessible by many other clients as well through some common mechanism, for example by using web browser or email. Additionally, the clients or users have no control over the application or underlying infrastructure, network server or operating system upon which these applications run.
- Platform as a Service (PaaS): In PaaS, the client is able to create their own desired application by using some programming language, linked libraries. These languages or libraries are supported by the vendor. After creating the user desired application, it is deployed on the server provided by the vendor. User has also the authority to configure its application or can change the configuration settings later on. The next Figure 2 shows the relationships of the clients and three service models defined bu NIST.

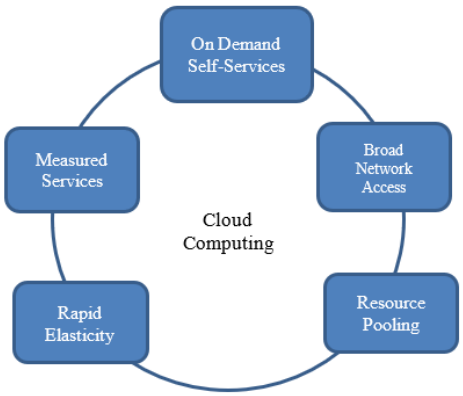


Figure 1. Cloud computing characteristics

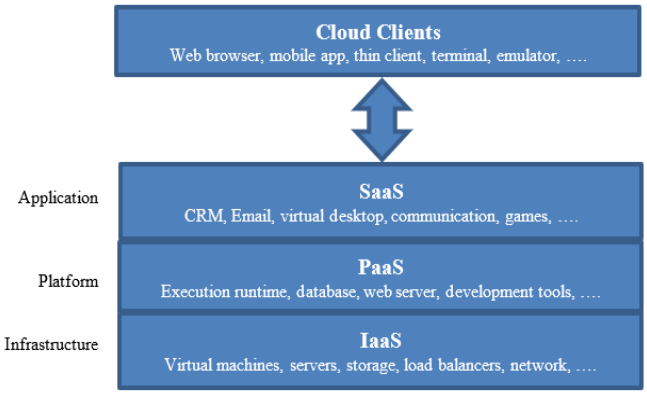


Figure 2. Different cloud service models

## 3. Related Works

Agarwal A et al. highlight the emergence of cloud computing along with its security concerns like data loss, data breaches, insecure APIs, account hijacking, denial of services [4, 5]. P Garg et al. have worked on different cloud security aspects like basic security which includes Cross site scripting attacks, SQL injection attacks, Man in the middle attacks [6]. Pradeep Kumar Sharma et al. also work for the security concerns of cloud like cost model charge [6, 7], service level agreements and issue of migration should be dealt. Naseer Amara et al. highlighted the security threats, architectural principles and cloud security attacks

with their techniques that can minimize the effects of malicious attacks (mitigation techniques) [8, 9]. Iqbal Ahmed et al. introduces green IT as a Service (GaaS), which is important for modern days sustainability concern [10]. S Ajoudaninan et al. said that following three parameters were the most crucial (a) data confidentiality (b) integrity (c) availability [11]. She proposed a new security model (CIA) [11], for cloud computing.

## 4. Factors Affecting Cloud Security

There are numerous key factors which may affect cloud computing performance because it is surrounded by many technologies, for example, load balancing, network, concurrency control, virtualization, operating system, database, memory management etc [12]. The main key factors which are affecting cloud performance are shown in Figure 3. The security factors of these technologies affecting the cloud computing are appropriate; for example, network which connects the cloud computing to the outer world has to be secured. Virtualization concept has to be carried out securely when mapping with the physical systems. Load balancing involves the handling of incoming requests traffic which sometimes overloads the server. Data mining algorithms can be applied to cope with malicious attacks.

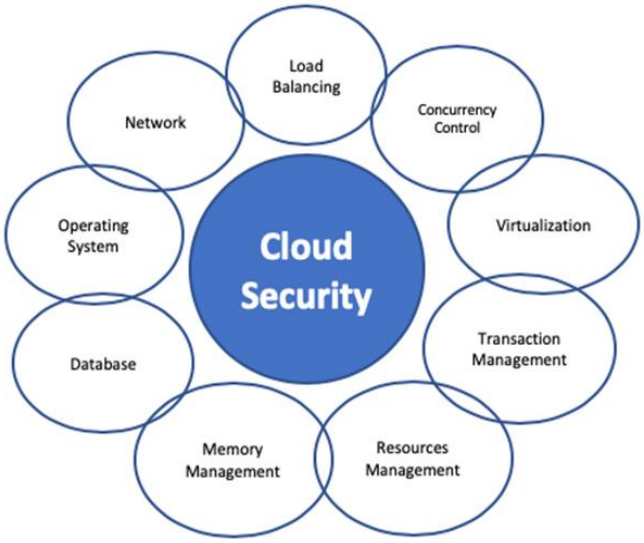


Figure 3. Factors affecting cloud security

## 5. Possible Threats Regarding Cloud Computing

Nowadays cloud computing is getting so much popularity that it is in the limelight of modern era. Along with its huge benefits cloud computing is facing much security issues which need considerable attention to resolve them for the betterment of this services. Following are the major concerns [13]:

- Outsourcing: in outsourcing the data, consumer might get lose the control. Some kind of appropriate mechanism is needed to prevent the cloud service provider (CSPs) to use the data against the consent of their clients.
- Multitenancy: cloud is a shared pool of resources. Protection of data must be taken into account while providing the multi-tenant environment.
- Service Level Agreements (SLA): a clear contract between the consumer and provider is needed. The main goal of agreements is to build trust.
- Heterogeneity: different cloud providers have different mechanism of data protection which leads to integration challenges.
- Server Downtime: downtime is the time in which the system starts responding to the client after some service failure. Downtime should be kept minimized and power backups must be installed to keep down time minimum.

- Backup: Data uploaded by the clients, should be backed up in case of any service failure. Cloud seller should mention in the SLAs that in case of any disaster what should be the remedy or solutions to such problems. There is very rare chance of whole system failure like flood etc.
- Data Redundancy: Data redundancy is a situation in which same data is being kept on two different places. In case of cloud computing, it can be understood as to provide copies of same data, systems or equipment to the clients, cloud provider should try to keep data redundancy minimum.

## 6. Solutions to Security Challenges in Cloud Computing

Security challenges in cloud computing need to be addressed properly. If appropriate solutions are not being provided, adoption of cloud environment becomes more difficult. Apart of adoption, data transmission and operation tend to become more tedious. Figure 4 elaborates that data protection and privacy is the most crucial factor among all [14]. Following are some solutions which needs to be considered while considering about cloud computing security challenges.

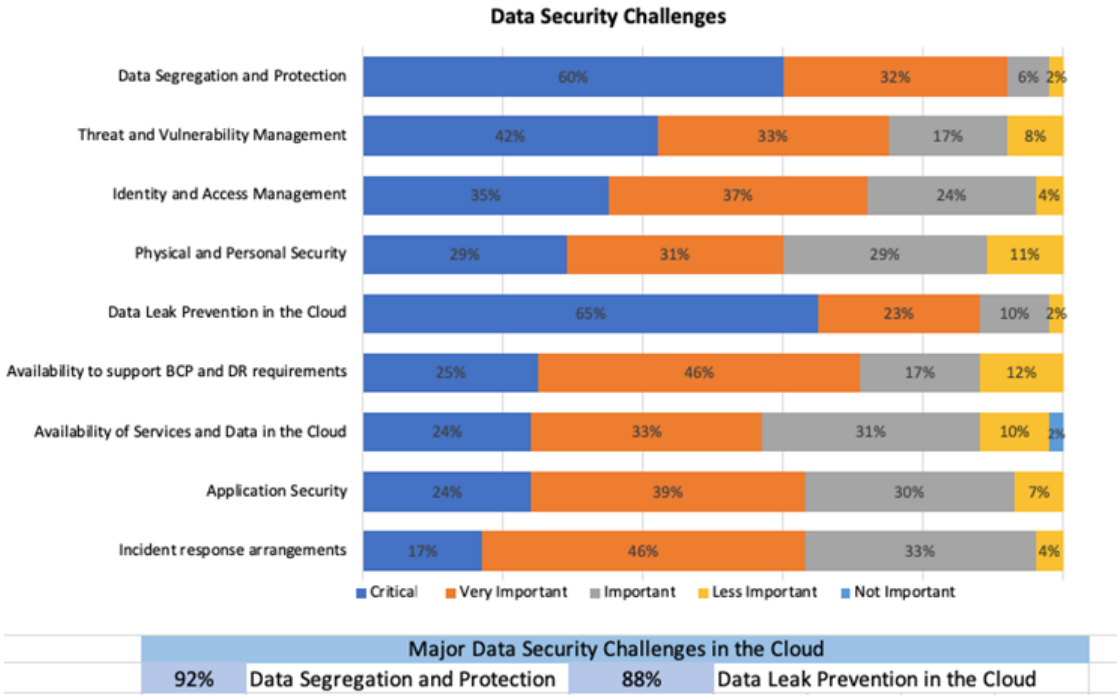


Figure 4. Data security challenges

### 6.1. Data Encryption

Encryption is said to be a better approach regarding data security. Data should be encrypted before sending it to cloud. Data owner can permit some particular members to have access to that data [14]. The file or data being sent to cloud should be encrypted first then before storing it on cloud it should be again encrypted by the cloud provider; the process is known as multistage encryption. It has been observed that combination of different encryption algorithms provides better encryption on data. Experimental results show that RSA+IDEA gives the higher performance of encryption in securing the data [15, 16].

### 6.2. Legal Jurisdiction

When it comes to understand and analyse the legal jurisdiction of cloud computing, the very basic aspects of cloud environment complicate the data protection, for example presence

of internet, virtualization, dynamically distributed data, multinational elements. Consumers normally do not know that where their data resides in cloud. For example, a client from India may be using a server deployed in USA, using an application which has been developed in Japan and storing his crucial data at a data centre which is physically located in Switzerland [17]. Therefore, the resource allocated to the consumers should be marked to make sure that data is segregated [18].

### 6.3. Distributed Denial of Service (DDoS)

Distributed Denial of Service is a kind of attack in which attacker creates some zombie machine by infecting the machine over the internet [19-22]. Then these infected machines are used to attack on victim. When attacks/traffic from so many infected machines are directed towards one victim, its resource like CPU, bandwidth and memory starts getting exhausted and particular resource becomes unavailable for consumers. To cope with this Deepali et al. [19] has introduced a layer named as fog layer which sites in between cloud server and user. All the requests made to server are filtered through this fog layer and DDoS attacks get minimized.

### 6.4. Digital Signature

Digital signature is powerful tool for securing data in cloud computing [23, 24]. P Rewagad et al. [25] has proposed a solution using digital signature to secure data along with Diffie Hellman key exchange with AES encryption algorithm. Diffie Hellman key exchange facility marks it useless if the key is hacked in transmission because it us useless without private key of user, which is confined to legitimate user only. This three-way mechanism which is proposed in that paper makes it harder to hack security system, therefore, protecting the data that resides in cloud.

## 7. Conclusion

This paper gave the overview of cloud computing, its various security aspects and key factors which are affecting the cloud security. Cloud consumer and provider should be sure that their cloud is fully secure and protected. Cloud computing is growing in every industry however it suffers from certain issues regarding security and protection which are hurdle in its adoption widely. Solutions to these problems have been suggested which can be used for better performance of cloud services in future.

## References

[1] Mell P, Grance T. The NIST Definition of Cloud Computing. NIST special publication 800-145. September 2011.
[2] Rashid Dar Ab, Ravindran D. A Comprehensive Study on Cloud Computing. *International Journal of Advance Research in Science and Engineering*. 2018; 7(4): 235-242.
[3] Mell P, Grance T. The NIST Definition of Cloud Computing, version 15. National Institute of Standards and Technology (NIST), Information Technology Laboratory. 2011.
[4] Simmon E. Evaluation of Cloud Computing Services Based on NIST 800-145. NIST special Publication. USA. 2018: 500-322
[5] Agarwal A, Siddharth S, Bansal P. *Evolution of Cloud Computing and related security concerns*. 2016 Symposium on Colossal Data Analysis and Networking (CDAN). Indore. 2016: 1-9.
[6] Chetan M B, Bhojannavar SS, Danawade VM. Cloud Computing: Research Activities and Challenges. *International Journal of Emerging Trends & Technology in Computer Science.* 2013; 2(5): 206-214.
[7] Grag P, Goel S, Sharma A. *Security Techniques for Cloud Computing Environment*. IEEE International Conference on Computing, Communication and Automation (ICCCA*)*. Greater Noida. 2017: 771-776.
[8] Sharma PK, Kaushik PS, Agarwal P, Jain P, Agarwal S, Dixit K*. Issues and Challenges of data security in a Cloud Computing Environment*. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). New York. 2017: 560-566.
[9] Amara N, Zhiqui H, Ali A. *Cloud Computing Security Threats and Attacks with their Mitigation Techniques*. 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE Explorer. Nanjing. 2017: 244-251.

[10] Ahmed I, Okumura H, Arai K. Identifying Green Services using GSLA for Achieving Sustainability in Industries. *International Journal of Advanced Computer Science and Applications (IJACSA)*. 2016; 7(9): 160-167.
[11] Ajoudanian Sh, Ahmadi MR. A Novel Data Security Model for Cloud Computing. *International Journal of Engineering and Technology*. 2012; 4(3): 326-329.
[12] Qadiree J, Maqbool IM. Solutions of Cloud Computing Security Issues. *International Journal of Computer Science Trends and Technology (IJCST).* 2016; 4(2): 38-42.
[13] Shahzad F. State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. *Procedia Computer Science*. 2014; 37: 357-362.
[14] Rao RV, Selvamani K. Data Security Challenges and its Solutions in Cloud Computing. *Procedia Computer Science*. 2015; 48: 204-209.
[15] Chennam KK, Muddana L, Aluvalu RK. *Performance Analysis of Various Encryption Algorithms for Usage in Multistage Encryption for securing data in Cloud*. 2nd IEEE International Conference on Recent trends in Electronics, Information & Communication Technology (RTEICT). India. 2017: 2030-2033.
[16] Yan Z, Deng RH, Varadharajan V. Cryptography Data Security in Cloud Computing. *Information Sciences*. 2017; 387: 53-55.
[17] Sony R, Rao SKD, Prasad DB. *Data Protection and Cloud Computing: A Jurisdictional Aspect*. Law Journal of Higher School of Economics. Annual review. 2013: 81-91.
[18] Harfoushi O, Alfawwaz B, and Ghatasheh NA. Data Security Issues and Challenges in Cloud Computing: A conceptual Analysis and Review. *Communications and Network* 2014; 6(1): 15-21.
[19] Deepali, Bhushan K. *DDoS Attack Defense Framework for Cloud using Fog Computing*. 2nd IEEE International Conference on Recent trends in Electronics, Information & Communication Technology (RTEICT). India. 2017: 534-538.
[20] Somani, Gaurav. DDoS attacks in cloud computing: Collateral damage to non-targets. *Computer Networks.* 2016; 109: 157-171.
[21] Paharia, Bhumika, Bhushan K. *DDoS Detection and Mitigation in Cloud Via FogFiter: A Defence Mechanism*. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). India. 2018: 1-7.
[22] Alqahtani, Sarra M, Rose F, Gamble. *DDoS Attacks in Service Clouds*. 48th Hawaii International Conference on System Sciences. USA. 2015: 5331-5340.
[23] Merkle, Ralph C. A Certified Digital Signature. CRYPTO*.* New York. 1989: 218-238.
[24] Grobauer, Bernd, Tobias Walloschek, Elmar Stocker. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy*. 2010; 9(2): 50-57.
[25] Rewagad P, Pawar Y. *Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing*. 2013 International Conference on Communication Systems and Network technologies. India. 2013: 437-439.